Shellcode Reflective DLL Injection (sRDI)

Loading DLL binaries reflectively and passing parameters to it

Reflective Loading (RL) vs Shellcode Reflective DLL Injection (sRDI)

- In Stephen Fewer's RL you have access to the source code of the DLL that you want to convert to become a Reflective DLL.
- But, what if you don't have the source code, what if you only have the binary?
- Solution: use SRDI – by Nick Landers
- He created a sRDI toolset to build sRDI Trojans
- https://www.netspi.com/blog/technical/adversary-simulation/srdi-shellcode-reflective-dll-injection/

Anatomy of an sRDI Trojan

1. Get current location in memory
2. Calculate and setup registers
3. Pass execution to Reflective Loader

4. Unpacks DLL and remaps sections
5. Call DllMain function
6. Call exported function
7. Pass user-data to exported function

Thank you